



## Installing Components

---

This chapter describes how to install the Cisco Subscriber Edge Services Manager (SESM) software and bundled components, including SPE. It includes the following topics:

- [Installation Requirements, page 5-1](#)
- [Obtaining the SESM Installation File and License Number, page 5-10](#)
- [Installation Privileges, page 5-12](#)
- [Installation Modes, page 5-12](#)
- [Installation and Configuration Parameters, page 5-14](#)
- [Installation Results, page 5-30](#)
- [Post-Installation Procedures, page 5-30](#)

## Installation Requirements

This section describes prerequisites to installing SESM. It includes the following topics:

- [Installation Platform Requirements, page 5-1](#)
- [RAM and Disk Space Requirements, page 5-2](#)
- [Java Software Considerations, page 5-2](#)
- [SSG and RADIUS Considerations, page 5-4](#)
- [LDAP Directory Configuration Requirements, page 5-4](#)
- [Dependencies among SESM Components, page 5-9](#)
- [Uninstalling a Previous Installation, page 5-10](#)

## Installation Platform Requirements

You can install SESM components on Sun Solaris, Linux, and Microsoft Windows platforms. See the [“Supported Hardware Platforms”](#) section on [page 1-12](#) for more information.

## RAM and Disk Space Requirements

Table 5-1 shows RAM and disk space requirements for a single instance of each component in SESM. These requirements are approximately the same on the Sun Solaris and the Windows NT platforms.

*Table 5-1 RAM and Disk Space Requirements*

Component Name	Disk Space (MB)	RAM
Jetty server	1.5	The Jetty server provides the J2EE application environment in which the SESM portal applications and CDAT execute. The application memory needs specified for NWSP and CDAT, below, include Jetty server usage.
SESM portal applications (NWSP, WAP, and PDA)	18.9	RAM requirements increase relative to the number of subscribers logged in. The following numbers are approximations: <ul style="list-style-type: none"> <li>In RADIUS mode, 64MB of JVM can service a maximum of 12,800 users.</li> <li>In LDAP mode, the DESS cache adds to the memory requirements. A JVM memory size of 64MB can service a maximum of 1800 users. See the <a href="#">“SPE Attributes” section on page 6-37</a> for cache size information.</li> </ul> See the <a href="#">“Memory Requirements and CPU Utilization” section on page 7-8</a> for memory utilization equations.
Captive Portal	2.0	The Captive Portal installation includes the Captive Portal and Message Portal applications.
RDP	4.2	The RDP uses the DESS cache. Memory requirements are roughly proportional to the login rate. See the <a href="#">“RDP Memory Requirements” section on page 7-10</a> for more information.
SPE components	1.9	N/A
CDAT	5.6	RAM requirements increase proportionally to the number of objects stored in the directory. For most directory sizes, the 64 MB requirements of the operating system (OS) and other system software should be sufficient for heavily populated directories.

## Java Software Considerations

A JRE Version 1.2.2 is bundled in the installation image. The installation process installs this bundled version if it cannot find a suitable version on the installation platform.

This section describes the SESM requirements regarding the Java Runtime Environment (JRE) and the Java Development Kit (JDK). The section includes the following topics:

- [Solaris Patch Requirements, page 5-3](#)
- [Installing the Bundled JRE, page 5-3](#)
- [Specifying an Existing JRE or JDK, page 5-3](#)
- [Specifying the JRE or JDK in the Startup Scripts, page 5-3](#)

- [Obtaining a JDK for SESM Web Development, page 5-4](#)

## Solaris Patch Requirements

On older Solaris platforms, you might need to apply Solaris operating system upgrades (patches). To determine if the machine requires patches, go to the Sun Microsystems Java site and start the process of downloading the JRE Version 1.2.2. After you log in, a list of download options appears, including the necessary patches for your operating system version. You should also download the README file, which contains instructions on how to apply the patches.

## Installing the Bundled JRE

The installation program determines for itself whether or not to install the bundled JRE Version 1.2.2 by doing the following:

1. It searches for a JDK Version 1.2.2 that is already installed.
2. Failing that, it searches for a JRE Version 1.2.2 or later that is already installed.
3. Failing that, it installs and uses the bundled JRE Version 1.2.2.

To search for an existing JDK or JRE, the installation program looks in the following locations:

- On Windows NT, it looks in the NT Registry for a referenced location.
- On Solaris, it looks in well-known locations. See the [“Searching for an Existing JDK or JRE” section on page 10-8](#) for a list of these locations.
- On Linux, it looks in well-known locations. See the [“Searching for an Existing JDK or JRE” section on page 10-8](#) for a list of these locations.

## Specifying an Existing JRE or JDK

On Windows NT, Solaris, and Linux, you can explicitly specify the location of a pre-installed JDK or JRE by starting the installation process on a command line and specifying the `javahome` parameter, as follows:

```
installImageName -is:javahome location
```

Where:

*installImageName* is the name of the downloaded SESM image.

*location* is the path name for the JRE or JDK directory. For example, `/usr/java1.2`.

## Specifying the JRE or JDK in the Startup Scripts

The installation process sets the location of the JDK or JRE in the startup files for the SESM portal applications, CDAT, and RDP.

If you change the location of the JDK or JRE after installation, make the corresponding change in the following two startup files:

- Generic startup script—This common script is executed by the startup scripts for the SESM portal applications and CDAT. It can also be used by the startup scripts for customized SESM portal applications.
- RDP startup script

Table 5-2 shows the path names of the startup scripts that you must change.

*Table 5-2 Startup Script Names*

Platform	Generic Startup Script	RDP Startup Script
Solaris and Linux	jetty/bin/start.sh	rdp/bin/runrdp.sh
Windows	jetty\bin\start.cmd	rdp\bin\runrdp.cmd

## Obtaining a JDK for SESM Web Development

A Java Development Kit (JDK) Version 1.2.2 or later must be installed on any system that will be used by web developers to create or modify the Java Server Pages (JSPs) for a customized SESM application. You can obtain JDK Version 1.2.2 or later from the Sun Java web page:

<http://java.sun.com/products/j2se>

On systems that will be used to customize an SESM application, we recommend that you install the JDK before you install SESM. In that way, the SESM installation program uses the JDK in the application startup scripts, rather than a JRE. The JDK is necessary for recompiling the changed JSPs. See the “[Recompiling a Customized JSP](#)” section on page 10-9 for more information.

If you install the JDK after installing SESM, then you must:

- Edit the SESM application start script to use the JDK.
- Ensure that the JDK\_HOME environment variable points to the directory into which you installed the JDK.

## SSG and RADIUS Considerations

The SESM installation program does not attempt to communicate with SSGs or RADIUS servers. Therefore, SSGs and RADIUS servers do not need to be configured and running for you to install SESM components.

However, you should be prepared to provide correct communication information about those network components during the installation. Otherwise, you must manually edit the configuration files at a later time for the SESM application to work correctly.

The installation program updates configuration files with information that you provide about the SSGs and RADIUS servers. [Table 5-5 on page 5-15](#) describes the configuration information that the installation program prompts you for.

## LDAP Directory Configuration Requirements

If you are installing SESM in LDAP mode, the installation program establishes communication with your LDAP directory, if possible. This section includes the following topics:

- [Advantages to Running an LDAP Directory During SESM Installation, page 5-5](#)
- [NDS Installation and Configuration Requirements, page 5-5](#)
- [iPlanet Installation and Configuration Requirements, page 5-7](#)

## Advantages to Running an LDAP Directory During SESM Installation

The LDAP directory does not need to be configured and running on the network for you to complete the Cisco SESM installation. However, it is advantageous if the directory is configured and running. If the installation program can communicate with the LDAP directory using the communication parameters that you provide, it can perform the following required tasks:

- Extend the directory schema with the SPE extensions. These extensions are the LDAP classes and attributes that will hold the SESM subscriber profiles, service profiles, and policy information.
- Install top-level RBAC objects that are required before administrators can log into CDAT to create additional RBAC objects and before you can install the SESM sample data.

If the installation program does not perform these tasks, you must do them at a later time before running an SESM web application or CDAT, as described in the [“Extending the Directory Schema and Loading Initial RBAC Objects”](#) section on page 6-40.

## NDS Installation and Configuration Requirements

This section describes how to install and configure Novell eDirectory Version 8.5 to work with SESM. On completion of these instructions, your NDS directory is configured as follows:

- Access to the NDS server is granted with the following distinguished name (dn):  
cn=admin.ou=sesm.o=cisco
- The following SESM container exists in the NDS directory:  
Tree name: sesm  
Server context: ou=sesm.o=cisco
- The following administrative user has all required permissions to update the NDS directory schema and also to create and modify objects in the SESM container.  
name: admin  
password: value you specified during the NDS installation
- The Allow Clear Text Passwords option is set to true (required).

To install and configure NDS to work with SESM, perform the following steps. These instructions assume that you are installing NDS on a Solaris machine.

- 
- Step 1** Log on as super user.
- Step 2** Create an NDS directory on the Solaris machine. A typical location is /usr/nds.
- Step 3** If you have an NDS tar file, place it into the directory you just created and expand it.
- Step 4** Run the installation file, which is located in:  
`/usr/nds/NDS8.5/Solaris/setup/nds-install`
- Step 5** The installation program prompts you to read and accept the License agreement.
- Step 6** The installation program prompts you to choose the components to install, as follows:  
1)NDS Server  
2)Administration Utilities  
3)Management Console for NDS (ConsoleOne)

In most cases, you should install all three components. To do so, enter:

1 2 3

**Step 7** The installation program prompts you for the location of the license files. Enter:

```
/usr/nds/NDS8.5/licensefiles
```




---

**Note** Refer to the NDS documentation if you do not have the license files.

---

**Step 8** The installation program installs the requested packages. Then it asks whether or not you want to install the Java Runtime Environment (JRE). The JRE is required for ConsoleOne, the NDS management console. If you do not already have a suitable JRE installed on the machine, enter:

```
yes
```

**Step 9** The installation program opens the NDS server configuration file (/etc/ndscfg.inp) in a text editor. Use the editor to enter the following required information. Use the values shown below to ensure compatibility with SESM installation and sample data defaults:

```
Admin Name and Context: cn=admin.ou=sesm.o=cisco
Tree Name: sesm
Create NDS Tree: YES
Server Context: ou=sesm.o=cisco
```

Two additional fields (server IP address and Database Files directory) are optional. You do not need to enter values for them.

**Step 10** Save the configuration file and quit the editor.

**Step 11** The installation program prompts you for a password for the admin user. Enter any password.




---

**Note** The SESM installation program prompts you for the administrator name (admin) and this password when you install the SPE component.

---

**Step 12** The installation program concludes by prompting you to manually edit two environment variables:

```
PATH=$PATH:/usr/ldaptools/bin
MANPATH=$MANPATH:/usr/ldaptools/man
```




---

**Note** The following instructions describe how to set the Allow Clear Text Passwords attribute. For SESM to work with NDS, this attribute must be enabled. This attribute allows transmission of bind requests that include passwords over nonencrypted connections. By default, only passwords exchanged over SSL connections are encrypted. The allow clear text password attribute is a property of the LDAP Group object of a server.

---

**Step 13** Start ConsoleOne. Run the following file:

```
/usr/ConsoleOne/bin/ConsoleOne
```

**Step 14** Authenticate to the NDS Directory as follows:

- In the tree, click the **NDS** icon.
- From the menu, choose **File** → **Authenticate**.
- In the Login window, type the password you entered for the admin user during installation. Accept the defaults displayed in the other fields in the login window. Click **Enter**.

Upon successful authentication, the .SESM. icon appears in the right panel.

**Step 15** Set the Allow Clear Text Passwords to **true**, as follows:

- In the left panel, expand the NDS tree to the sesm object level:

```
NDS
 .SESM.
 cisco
 sesm
```

- In the left panel, click **SESM** to select it.
- In the right panel, right-click the **LDAP Group object**.
- Choose **Properties** from the pop-up menu.
- In the **General** tab, in the middle of the window, check the **Allow Clear Text Passwords** option.
- Click **Apply**. Then click **Close**.

**Step 16** Exit ConsoleOne and proceed to the SESM installation.

---

## iPlanet Installation and Configuration Requirements

This section describes how to install and configure iPlanet to work with SESM. On completion of these instructions, your iPlanet directory is configured as follows:

- Access to the server is granted with the following distinguished name (dn):  
uid=admin.ou=sesm.o=cisco
- The following SESM container exists in the directory:  
Tree name: sesm  
Server context: ou=sesm.o=cisco
- The following administrative user has all required permissions to update the directory schema:  
name: Directory Manager  
password: value you specify during the iPlanet installation
- The following administrative user has all required permissions to create and modify objects in the SESM container.  
name: admin  
password: value you specify during the iPlanet installation

To install and configure iPlanet to work with SESM, perform the following steps. These instructions assume that you are installing iPlanet Version 5.0 on a Solaris machine.

---

**Step 1** Log on as superuser.

**Step 2** If you have a tar file, expand it.

**Step 3** Execute the setup file. Follow the instructions in the setup program.

**Step 4** When the program displays the following prompt, select the **iPlanet Servers** option.

- ```
1. iPlanet Servers
   Installs iPlanet Servers with the integrated iPlanet Console onto your computer.
2. iPlanet Console
   Installs iPlanet Console as a stand-alone Java application on your computer.
```

- Step 5** In response to subsequent prompts to install components, select **all components**.
- Step 6** When the program displays the following prompt, we recommend that you enter the standard port **389**, rather than accepting the random default port. You must know this port number later in this procedure and also during SESM installation.
- ```
Directory server network port[nnnnn]: 389
```
- Step 7** At the following prompt, accept the default value of **admin**.
- ```
iPlanet configuration directory server
administrator ID [admin]:
Password:
Password (again):
```
- Enter the password of your choice. This user name and password has privileges to update the directory schema. You must enter this admin ID and password later in this procedure and also during SESM installation.
- Step 8** When the program displays the following prompt, enter the value **o=cisco**.
- ```
Suffix [dc=]:o=cisco
```
- Step 9** When the program displays the following prompt, accept the default value of **Directory Manager**.
- ```
Directory Manager DN [cn=Directory Manager]:
Password:
Password (again):
```
- Enter the password of your choice. This user name and password has privileges to add objects to the cisco container you created in the previous step. You must enter this Directory Manager DN and password later in this procedure and also during SESM installation.
- Step 10** When the program displays the following prompt, enter any port number. The configuration examples later in this procedure use the value 390.
- ```
Administration port [15197]:390
```
- Step 11** When the program displays the following prompt, enter a user name or accept the default value (root).
- ```
Run Administration Server as [root]:
```
- The installation process is complete. After successful installation, the iPlanet servers start automatically.
- Step 12** Change the directory to:
- ```
/usr/iplanet/servers
```
- Step 13** Execute the following program:
- ```
startconsol
```
- A logon window appears.
- Step 14** Log on as follows:
- ```
User ID:cn=Directory Manager
Password:
AdminURL:http://hostname:390
```
- The iPlanet Console window appears.
- Step 15** Expand the folders in the iPlanet Console window until the Directory Server object appears. Select **Directory Server** and click **Open** at the top right corner of the window.
- An iPlanet Directory Server window appears.



- Step 16** Right-click the **cisco** folder. Choose **New** → **Org Unit** from the pop-up menu.
- Step 17** In the Name field, enter **sesm** and click **OK**.  
Name: sesm
- Step 18** Right-click the **sesm** object. Choose **New** → **User** from the pop-up menu. A Create New User window appears.
- Step 19** Enter appropriate values. In the UserID field, enter **admin**. Click **OK**.  
First Name:  
Last Name:  
Common Name:  
UserID: admin  
Password:
- Step 20** Right-click the **sesm** object. Choose **Set Access Permissions** from the pop-up menu. The Manage Access Control window for ou=sesm,o=cisco appears.
- Step 21** Click **New**. The Edit ACI window for ou=sesm,o=cisco appears.
- Step 22** Enter any value for ACIName and click **Add**.  
ACI Name :aciAdmin  
  
The Add User & Group window appears.
- Step 23** Enter the following value in the search field and click **Search**:  
**admin**  
  
The admin user appears in the top window.
- Step 24** Select **admin** and click **Add**. The admin user appears in the bottom window. Click **OK**.
- Step 25** Click **Targets**. Click **This Entry**. Click **OK**.
- Step 26** Click **OK** in the Manage Access Control window.
- Step 27** Exit iPlanet and proceed to the SESM installation.
- 

## Dependencies among SESM Components

You can install all SESM components together on the same machine (a typical installation), or you can install some components separately in a distributed manner (a custom installation). [Table 5-3](#) describes components that must be installed together on the same machine. The installation program detects these dependencies and enforces the correct installation.

*Table 5-3 Component Dependencies in a Distributed Installation*

SESM Mode	Component Dependencies
RADIUS mode	<ul style="list-style-type: none"> <li>An SESM portal application requires a J2EE server (for example, jetty) on the same machine.</li> </ul>
LDAP mode	<ul style="list-style-type: none"> <li>An SESM portal application requires a J2EE server (for example, jetty) and the SPE component on the same machine.</li> <li>CDAT requires a J2EE server (for example, jetty) and the SPE component on the same machine.</li> <li>RDP requires the SPE component on the same machine.</li> </ul>

## Uninstalling a Previous Installation

Use the uninstall utility provided with the SESM product to remove a previous installation. The uninstall utility is located in the following directory:

```
installDir
  _uninst
    uninstall.bin or uninstall.exe
```

The uninstall utility does the following:

- Lets you choose the components to uninstall.
- Verifies the installation directory that is being uninstalled.
- Uninstalls the SESM components. It does not remove the installation directory, only the contents under the installation directory.

After running the uninstall utility, you can safely reinstall one or more SESM components into the same directory.



### Note

Do not uninstall SESM by manually deleting the contents of the installation directory. If you do so, and then attempt a reinstall into the same directory, the installation might not be complete. If the installation is incomplete, see the [“Incomplete Installation or Files Installed in Incorrect Directory”](#) section on page 10-10 for information.

## Obtaining the SESM Installation File and License Number

The installation images for SESM are available from the product CD-ROM or from the Cisco web site. This section includes the following topics:

- [Obtaining a License Number, page 5-11](#)
- [Downloading from the Cisco Web Site, page 5-11](#)
- [Uncompressing the Image, page 5-11](#)

## Obtaining a License Number

The SESM installation program installs evaluation and licensed versions of SESM:

- **Evaluation**—The evaluation options do not require a license number and do not have an expiration period. An evaluation installation provides full software functionality. You can install a RADIUS mode evaluation or an LDAP mode evaluation.
- **Licensed**— You must install a licensed version using a license number before deploying SESM in a production environment.

The license number is available on the License Certificate that is shipped with a purchased product. If you have purchased the product and have not yet received the CD-ROM and License Certificate, you can choose the evaluation option during installation. However, be sure to reinstall using your license number when you receive the certificate.

The license number is important when you are requesting technical support for SESM from Cisco. After installation, you can see your license number and the software version in the `licensenum.txt` file under the installation directory.

## Downloading from the Cisco Web Site

If you purchased a contract that allows you to obtain the SESM software from the Cisco web site, follow these procedures:

- 
- Step 1** Open a web browser and go to:  
`http://www.cisco.com`
  - Step 2** Click the **Login** button. Enter your Cisco **user ID** and **password**.  
To access the Cisco images from the CCO Software Center, you must have a valid Cisco user ID and password. See your Cisco account representative if you need help.
  - Step 3** Under Service and Support, click **Software Center**.
  - Step 4** Click **Web Software**.
  - Step 5** Click **Cisco Subscriber Edge Services Manager**.
  - Step 6** Download the appropriate image based on the platform you intend to use for hosting the SESM web application.
- 

## Uncompressing the Image

Copy and uncompress the tar or zip file to a temporary directory. When you uncompress the file, the results are:

- The installation executable file—A `.bin` or `.exe` file, depending on the platform you are using.
- Files used for a silent mode installation—These are `.iss` and `.properties` files. See the [“Installing Using Silent Mode”](#) section on page 5-14 for information about silent mode.

Table 5-4 shows the names of the compressed and executable files.

**Table 5-4** *Installation Image Filenames*

Platform	Compressed Filename	Executable Installation Filename
Solaris	sesm-3.1.3-pkg-sol.tar	sesm_sol.bin
Linux	sesm-3.1.3-pkg-linux.tar	sesm_linux.bin
Windows NT	sesm-3.1.3-pkg-win32.zip	sesm_win.exe

## Installation Privileges

You must log on as a privileged user to perform the installation. In addition, you must have write privileges to the directory in which you intend to load the solution components.

The installation program writes to parts of the file system or Windows registry that are only accessible to a privileged user. The outcome of the installation is unpredictable if you are not privileged.

Log on as a privileged user as follows:

- On Solaris and Linux—Run the installation program as root.
- On Windows NT—Run the installation program as a member of the Administrators group.

## Installation Modes

You can install SESM using the following installation modes:

- **Installing Using GUI Mode**—An interactive installation method that communicates with you by displaying interactive windows. You use the mouse and the keyboard to provide input during the installation.  
To run the installation in GUI mode, execute the installation image. No special arguments are required.
- **Installing Using Console Mode**—A text-only, question and answer interactive installation method.  
To run the installation in console mode, use the `-console` argument on the command line when you execute the installation image.
- **Installing Using Silent Mode**—A text-only noninteractive method. This mode, also known as batch mode, is useful for multiple installs. Before you start the installation process, you prepare files that contain your installation and configuration information. The installation program obtains all input from the response file.  
To run the installation in silent mode, use the `-option fileName` argument on the command line when you execute the installation image.

The following sections provide more details about performing installations in these modes.

## Turning On the Installation Logging Feature

The `-log` option on the installation command line turns on the installation logging feature.

- On Solaris:

```
solaris> sesm_sol.bin -log location @ALL
```

Where:

*location* can be `#` to send logging messages to the console or a filename.

`@ALL` indicates to log all messages, which is the recommended procedure.

- On Windows NT:

```
C:\> sesm_win.exe -options -log location @ALL
```

Where:

*location* can be `#` to send logging messages to the console or a filename.

`@ALL` indicates to log all messages, which is the recommended procedure.

## Installing Using GUI Mode

GUI mode is the default installation mode. To run in this mode, execute the installation image. No options are required.

- On Solaris, change directories to the location of the installation image, and enter the image name. For example:

```
solaris> sesm_sol.bin
```

- On Windows NT, double-click the installation image filename. Alternatively, open a command prompt window, change directories to the location of the image, and enter the image name. For example:

```
C:\> sesm_win.exe
```

## Installing Using Console Mode

To run in console mode, use the `-console` option on the command line.

- On Solaris, change directories to the location of the installation image, and enter the following command:

```
solaris> sesm_sol.bin -console
```

- On Windows NT, open a command prompt window, change directories to the location of the image, and enter the following command:

```
C:\> sesm_win.exe -console
```

## Installing Using Silent Mode

To run in silent mode, you must first prepare the configuration information normally gathered during the installation process in two files:

- InstallShield properties file (.iss file)—This file defines values related to the installation process. It includes the name of the .properties file. This file is specified as an argument on the command line when you start the installation process.
- Java system properties file (.properties file)—This file defines values related to application configuration.

Examples of the .iss and .properties files are included in the installation download. You must modify both files to match your requirements before you start the installation.

To prepare for silent mode:

---

**Step 1** Open the .properties and .iss files in any text editor.




---

**Note** Before you begin, you might need to obtain write access to the files.

---

**Step 2** Edit the values for each parameter in the file. [Table 5-5 on page 5-15](#) describes each parameter. Save and close the file.

**Step 3** To turn on the installation logging feature for a silent mode installation, open the .iss file in any text editor. Remove the first pound sign (#) from the following line:

```
# -log # @all
```

**Step 4** Save and close the file.

---

To run in silent mode, use the `-options` option on the command line, as follows:

```
imageName -options issFileName
```

Where:

*imageName* is the name of the downloaded installation image.

*issFileName* is the name of the install shield properties file you prepared.

For example:

- On Solaris, change directories to the location of the installation image, and enter the following command:

```
solaris> sesm_sol.bin -options mysesm.iss
```

- On Windows NT, open a command prompt window, change directories to the location of the image, and enter the following command:

```
C:\> sesm_win.exe -options mysesm.iss
```

## Installation and Configuration Parameters

[Table 5-5](#) describes the installation and configuration parameters to enter during the installation process. Use the Value column in the table to record your planned input values.

You can change the value of any configuration parameter later by editing configuration files, as described in Chapter 4. You cannot change the values of the general installation parameters identified in the first part of the table.

*Table 5-5 SESM Installation and Configuration Parameters*

Category	Input Summary	Explanation	Value
General installation parameters	Installation type and license number	<p>Choose the type of installation:</p> <ul style="list-style-type: none"> <li>• <b>RADIUS Evaluation</b>—Choose this option to evaluate SESM in a RADIUS deployment. You do not need a license number, there is no expiration time associated with the evaluation, and the functionality is the same as that of licensed mode.</li> <li>• <b>LDAP Evaluation</b>—Choose this option to evaluate SESM in an LDAP deployment. You do not need a license number, there is no expiration time associated with the evaluation, and the functionality is the same as that of licensed mode.</li> <li>• <b>Licensed</b>—If you purchased an SESM license, choose this option and enter the license number provided by Cisco.</li> </ul> <p>The installation program interprets the license number you enter and proceeds to install either RADIUS or LDAP mode components, whichever matches the license you purchased. A RADIUS mode license will not allow you to install the LDAP-specific components, such as CDAT and RDP.</p> <p><b>Note</b> Obtain your SESM license number from the License Certificate shipped with the CD-ROM or otherwise provided to you by your Cisco account representative. If you have not yet received a Certificate, choose one of the Evaluation modes.</p> <p>The licensenum.txt file in your root installation directory records your license number and the software version number you installed. This information is important when you access Cisco technical support for this product.</p>	
	License agreement	<p>Read the displayed license agreement to ensure that you agree with the terms of the license. You must accept the agreement to proceed with installation.</p>	
	Installation directory	<p><b>Note</b> You must have write privileges to the installation directory.</p> <p>To specify the installation directory, you can accept the displayed default installation directory, click <b>Browse</b> to find a location, or type the directory name in the box.</p> <p>The default installation directories are:</p> <ul style="list-style-type: none"> <li>• On Solaris and Linux: /opt/cisco/sesm_3.1.3</li> <li>• On Windows NT: C:\Program Files\cisco\sesm_3.1.3</li> </ul>	

Table 5-5 *SESM Installation and Configuration Parameters (continued)*

Category	Input Summary	Explanation	Value
General installation parameters (continued)	Setup type	<p>Select one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Typical</b>—If you are installing a RADIUS evaluation or a RADIUS license, the Typical installation includes the following components: <ul style="list-style-type: none"> <li>– Web Applications—Includes the NWSP, WAP, and PDA sample applications and the SESM core model.</li> <li>– Jetty—Includes the Jetty web server, the JMX server, and JNDI.</li> </ul> </li> </ul> <p>If you are installing an LDAP evaluation or LDAP license, the Typical installation includes the following components:</p> <ul style="list-style-type: none"> <li>– Web Applications—Includes the NWSP, WAP, and PDA sample applications and the SESM core model.</li> <li>– Jetty</li> <li>– SPE</li> <li>– RDP</li> <li>– CDAT</li> </ul> <ul style="list-style-type: none"> <li>• <b>Custom</b>—Allows you to choose the components to install and configure from a checklist. Choose this option to: <ul style="list-style-type: none"> <li>– Include the SESM captive portal solution in your installation.</li> <li>– Reinstall one of the components.</li> <li>– Distribute the SESM components among different workstations.</li> </ul> </li> <li>• <b>Demo</b>—Installs and configures the NWSP, WAP, and PDA applications to run in Demo mode. The configuration files are not set up to communicate with an SSG, a RADIUS server, or an LDAP directory. Choose this option when those components are not available.</li> </ul> <p>The difference between a demo installation and a typical installation is the contents of the configuration files. In addition, a demo installation does not install the SPE component.</p>	



Table 5-5 *SESM Installation and Configuration Parameters (continued)*

Category	Input Summary	Explanation	Value
Web server configuration	Web Application Port Number	<p>Specify the port on which the container (the J2EE web server) for the SESM portal applications will listen for HTTP requests from subscribers. The installation program updates the application startup scripts for NWSP, WAP, and PDA to use this value. If you want to run these applications simultaneously, you must edit the start scripts to ensure that each application uses a different port.</p> <p>The displayed default value is port 8080.</p> <p><b>Tip</b> Each web server running on the same machine must listen on its own unique port. If another web server or another instance of the SESM portal application is listening on 8080, change this value.</p> <p>The application startup script uses the application port number to derive two other port numbers:</p> <ul style="list-style-type: none"> <li>A secure socket listener (SSL) port is derived as follows:  <math display="block">\text{application port} - 80 + 443</math> <p>When the application port is 8080, the SSL port is:  <math display="block">8080 - 80 + 443 = 8443</math></p> </li> <li>A management console port is derived as follows:  <math display="block">\text{application port} + 100</math> <p>When the application port is 8080, the management port is:  <math display="block">8080 + 100 = 8180</math></p> </li> </ul>	

**Note** If you are installing SESM in Demo mode, you are finished with the installation.

Table 5-5 *SESM Installation and Configuration Parameters (continued)*

Category	Input Summary	Explanation	Value
SESM to SSG communication  <b>Tip</b> Use the <b>show run</b> command on the SSG host device to determine how SSG is configured.	SSG port number	Specify the port that SSG uses to listen for RADIUS requests from an SESM application. This value must match the value that was configured on the SSG host with the following command:  <code>ssg radius-helper authenticationPort</code>  The default value is 1812.	
	SSG shared secret	Specify the shared secret used for communication between SSG and an SESM application. This value must match the value that was configured on the SSG host with the following command:  <code>ssg radius-helper key secret</code>  The default value is <code>cisco</code> .	
	SSG port bundle size	Enter the number of bits that SSG uses for port bundling when the port-bundle host key feature is enabled. This value must match the value that was configured on the SSG host with the following command:  <code>ssg port-map length</code>  We recommend using the value 4.  A value of 0 indicates that the SSG is not using the port-bundle host key mechanism.  <b>Note</b> The port-bundle host key feature was introduced in Cisco IOS Release 12.2(2)B. If you are using an earlier release, use a value of 0 in this field.  The default value is 0.	

When the port bundle size is 0, you must map SSGs to client subnets. The following category of parameters lets you map one client subnet for one SSG. You must manually edit the configuration file to:

- Map additional non-host key SSGs,
- Add more client subnets to this SSG, or
- Override the global values you specified in the previous category.

See the [“Associating SSGs and Subscriber Requests” section on page 6-25](#) for more information.

One non-host key SSG	SSG address	Enter the host name or IP address of the SSG host.	
	Client subnet	Enter one client subnet address handled by this SSG. For example, 177.52.0.0.	
	Subnet mask	Enter the mask that can be applied to subscriber IP addresses to derive their subnet. For example, 255.255.0.0.	

**Note** If you are installing SESM in LDAP mode, skip the following two categories and continue with the “Directory server information” category later in this table.

Table 5-5 *SESM Installation and Configuration Parameters (continued)*

Category	Input Summary	Explanation	Value
SESM to RADIUS server communication	Primary AAA server IP	Enter the IP address or the host name of the primary RADIUS server.	
	Primary AAA server port	Enter the port number on the primary RADIUS server host that the RADIUS server listens on. The default is 1812.	
	Secondary AAA server IP	Enter the IP address or the host name of the secondary RADIUS server. If you are not using a secondary RADIUS server, enter the same value used for the primary server.	
	Secondary AAA server port	Enter the port number on the secondary RADIUS server host that the RADIUS server listens on. If you are not using a secondary RADIUS server, enter the same value used for the primary server.	
	Shared secret	Enter the shared secret used between the RADIUS server and SESM. If you are using a primary and a secondary server, the shared secret must be the same for both servers. The default value is <code>cisco</code> .	
Passwords	Service password	Enter the password that the SESM application uses to request service profiles from RADIUS. It must match the service password values used in the service profiles in the RADIUS database.  This password must also match the value that was configured on the SSG host with the following command:  <code>ssg service-password password</code>  The service-password value must be the same on all of your SSGs.  The default value is <code>servicecisco</code> .	
	Service group password	Enter the password that the SESM application uses to request service group profiles from RADIUS. It must match the service group password values used in the service group profiles in the RADIUS database.  The default value is <code>groupcisco</code> .	

**Note** If you are installing SESM in RADIUS mode, you are finished with the installation.

Table 5-5 *SESM Installation and Configuration Parameters (continued)*

Category	Input Summary	Explanation	Value
Directory server information	Directory address	Enter the IP address or the host name of the system on which the directory server is running.	
	Directory port	Enter the port on which the directory server listens.	
	Directory admin user	Enter a user ID that has permissions to extend the directory schema. Use cn or uid as appropriate. For example: <ul style="list-style-type: none"> <li>For NDS, enter: cn=admin, ou=sesm, o=cisco</li> <li>For iPlanet, enter: uid=Directory Manager, ou=sesm, o=cisco</li> </ul>	
	Directory admin password	Enter the password for the directory administrator. This is the password you entered during directory installation and configuration. For example: <ul style="list-style-type: none"> <li>For NDS, enter the password you specified for the admin user during installation.</li> <li>For iPlanet, enter the password you entered for the Directory Manager user during installation.</li> </ul>	
	Meta Schema	Choose the component in distinguished name (dn) that your LDAP directory uses to allow access to the directory. <ul style="list-style-type: none"> <li>common name (cn)—NDS, for example, uses cn.</li> <li>unique identifier (uid)—iPlanet, for example, uses uid.</li> </ul> <p><b>Note</b> The SESM sample data uses cn. If you choose uid, you must edit the sample data before loading it into the directory. See the <a href="#">“Loading Sample Data and Logging into CDAT for the First Time”</a> section on page 6-41.</p>	

**Note** The installation program attempts to access the directory server, using the information you provided. If access is unsuccessful, the installation program displays a window with the header “Warning—Please confirm these options.” Verify the information you entered and also verify that the directory server is running. If the directory is not running, you can continue the installation of SPE components by clicking the **Ignore** button on the warning window. However, if you click **Ignore**, the installation program cannot update the directory for SESM use. You must perform the updates at a later time before you run SESM web applications or CDAT. See the [“Extending the Directory Schema and Loading Initial RBAC Objects”](#) section on page 6-40 for instructions.

Table 5-5 *SESM Installation and Configuration Parameters (continued)*

Category	Input Summary	Explanation	Value
Directory container information	Directory container	<p>Enter the organization and organizational unit that will hold the SESM service, subscriber, and policy information. Use the following format:</p> <pre>ou=orgUnit,o=org</pre> <p>For example, the installation program's default values are:</p> <pre>ou=sesm,o=cisco</pre> <p>The above defaults are the values used in the sample data file that is shipped with CDAT.</p>	
	Directory user ID	<p>Enter a user ID that has permissions to access and create objects in the organization and organizational unit named above. Use cn or uid as appropriate. For example:</p> <ul style="list-style-type: none"> <li>For NDS, the container administrator is the same as the directory administrator you entered on the previous window: <pre>cn=admin,ou=sesm,o=cisco</pre> </li> <li>For iPlanet, the container administrator is not the same. You created this directory administrator after installation. <pre>uid=yourAdmin,ou=sesm,o=cisco</pre> </li> </ul>	
	Directory password	Enter the password associated with the directory user ID.	
<p><b>Note</b> The installation program attempts to access the container using the information you provided. If it is unsuccessful, a warning message appears, as described in the previous note.</p>			
CDAT	CDAT port number	<p>Enter the port number on which the CDAT web server will listen.</p> <p>The default is 8081.</p>	

Table 5-5 *SESM Installation and Configuration Parameters (continued)*


Category	Input Summary	Explanation	Value
RDP Configures RDP to SSG communication	IP address	<p>Enter the IP address or host name of the RDP.</p> <p> <b>Caution</b> This value must be a real IP address to which the SSG host device can route. You cannot use the values localhost or 127.0.0.1.</p>	
	Port number	<p>Enter the port on which the RDP will listen.</p> <p>The default is 1812.</p>	
	Shared secret	<p>Enter the shared secret to be used for communication between the SSGs and RDP when the restricted client feature is turned off. This value must match the value configured on the SSG host devices, using the following command:</p> <pre>radius-server key SharedSecret</pre> <p>When the restricted client feature is turned off, the shared secret must be the same on all SSGs.</p> <p>When the restricted client feature is turned on, this attribute is ignored. Instead, you configure a specific shared secret for each client (each SSG). See the RDP MBean description in <a href="#">Table 6-6 on page 6-32</a> for more information.</p> <p>The next set of prompts from the installation program lets you choose whether to turn the restricted client feature on or off.</p> <p>The default shared secret value is <code>cisco</code>.</p>	
	Service password	<p>Enter the password that RDP uses to request service profiles from the directory. This value must match two other configured values:</p> <ol style="list-style-type: none"> <li>1. This password must match the value that was configured on the SSG host with the following command: <pre>ssg service-password password</pre> <p>The service-password value must be the same on all the SSGs that communicate with this RDP server.</p> </li> <li>2. This value must also match the service password value you entered for the SESM portal. See the SESM “<a href="#">Passwords</a>” section on <a href="#">page 5-19</a>.</li> </ol> <p>The default value is <code>servicecisco</code>.</p>	
Group password	<p>Enter the password that RDP uses to request service group profiles from the directory.</p> <p>This password must match the group password value you entered for the SESM portal. See the SESM “<a href="#">Passwords</a>” section on <a href="#">page 5-19</a>.</p> <p>The default value is <code>groupcisco</code>.</p>		

Table 5-5 *SESM Installation and Configuration Parameters (continued)*

Category	Input Summary	Explanation	Value
	Next hop password	<p>Enter the password that SSG uses to request next hop tables from RDP.</p> <p>This password must match the value that was configured on the SSG host with the following command:</p> <pre>ssg next-hop download nextHopTableName password</pre> <p>The service-password value must be the same on all of the SSGs that communicate with this RDP server.</p> <p>The default is <code>nexthopcisco</code>.</p>	
RDP Options	Proxy mode	<p>Choose this option to run RDP in proxy mode. RDP has two modes:</p> <ul style="list-style-type: none"> <li>Proxy mode—In this mode, RDP forwards authentication requests to a RADIUS server. RDP uses the SPE API to send authorization requests to the directory.</li> <li>Non-proxy mode—In this mode, RDP performs authentication based on information it obtains from the directory. RDP uses the SPE API to send authorization requests to the LDAP directory.</li> </ul>	
	Add services	<p>Choose this option if you want the SSG to perform automatic connections to services when a subscriber's profile includes the autoconnect attribute. When you choose this option, RDP includes the subscriber's service list and related information in replies to SSG. The service information consumes memory on the SSG device.</p> <p>Do not choose this option if space is a consideration on the SSG device. Instead, you can configure the SESM application to initiate automatic connections. See the <a href="#">“autoConnect” section on page 6-20</a> for more information.</p>	
	Add client	<p>Choose this option if you want to turn on the RDP restricted client feature, which allows RDP to service requests only from a preconfigured list of clients. The RDP clients are SSGs.</p> <p>If you check this option, the installation program prompts for configuration information for one client. You must manually edit the <code>rdp.xml</code> file to add more clients.</p> <p>If you do not check this option, the RDP accepts requests from any client (any SSG).</p>	

Table 5-5 *SESM Installation and Configuration Parameters (continued)*

Category	Input Summary	Explanation	Value
If you choose the Add client option, the installation program prompts you for the following information about one RDP client. To add more clients, manually edit the rdp.xml file			
RDP Client	Client name	Identifies the SSG. This value is used in logs and traces and does not have to match any other configured value.	
	Client IP address	The IP address of the SSG.	
	Shared Secret	The shared secret used for SSG to RDP communication. This value must match the value configured on the SSG devices, using the following command:  <code>radius-server key SharedSecret</code>	

If you are doing a Custom installation and you checked the Captive Portal item, the installation program prompts you for the following information.

**Note** Captive portal installation parameters must match TCP redirect configuration values on the SSG. The easiest way to ensure that values match in both places is to accept all of the default values presented during SESM captive portal installation. Then configure the SSG based on the example captiveportal/config/ssgconfig.txt file. See [Chapter 8, “Deploying a Captive Portal Solution,”](#) for more information.

Captive Portal Server Configuration	Captive portal address	Enter the IP address of the hardware platform on which you are installing the captive portal solution.	
	Captive portal port number	Enter the port number on which the first listener in the captive portal web server will listen.  This installation program sets up the captiveportal.jetty.xml file to create 7 listeners in the web server, as follows: <ul style="list-style-type: none"> <li>• 1 Subscriber redirection listener</li> <li>• 1 Initial logon redirection listener</li> <li>• 1 Advertising redirection listener</li> <li>• 1 Default service redirection listener</li> <li>• 3 Service redirection listeners</li> </ul> Later in this installation procedure, you are prompted for a port number for each of these listeners. The port you enter now is used as the default value for the first listener.  <b>Note</b> If you use the same port number for more than one listener, some redirections will not work.  Default: 8090	
	Install Message Portal	Choose this option if you want to install the Message Portal application. The Message Portal application is an example of an SESM portal that provides content for: <ul style="list-style-type: none"> <li>• Initial logon redirections</li> <li>• Advertising redirections.</li> </ul> For those redirection types, the default URIs displayed later in this installation procedure refer to pages in the Message Portal application.	



Table 5-5 *SESM Installation and Configuration Parameters (continued)*

Category	Input Summary	Explanation	Value
If you choose the Message Portal option above, the installation program prompts you for the following information:			
Message Portal Server Configuration	Message Portal Port Number	Enter the port number on which the Message Portal web server will listen. The Message Portal web server has one listener. Default: 8085	
	Redirect after message page	Choose this option if you want the Message Portal application to redirect the subscriber to the originally requested URL after the message duration time elapses. If you do not choose this option, the subscriber must enter an URL to leave the message page. Default: true	
Portal for service and error redirections	Host	Enter the host name or IP address of the web server for the NWSP or other application that will respond to: <ul style="list-style-type: none"> <li>Unauthenticated user redirection</li> <li>Default unconnected service redirection</li> <li>Specific unconnected service redirections</li> <li>Error handling due to captive portal misconfiguration (if a port has been used which is not configured for redirection).</li> </ul> This value becomes the default value for the serviceportal.host system property in the captiveportal.xml file.	
	Port	Enter the port number on which the web server named above will listen.  This value becomes the default value for the serviceportal.port system property in the captiveportal.xml file. Default: 8080	

Table 5-5 *SESM Installation and Configuration Parameters (continued)*

Category	Input Summary	Explanation	Value
Unauthenticated User Redirection	Enable	Check this box to configure unauthenticated user redirections.	
	Port In	<p>Enter the port that the web server for the Captive Portal application will listen on for unauthenticated user redirections received from the SSG. The installation program displays the value that you entered earlier in the Captive Portal Port Number field. You can accept this default value.</p> <p><b>Note</b> You must configure the SSG TCP redirect feature to send unauthenticated user redirections to this port.</p> <p>Default: 8090</p>	
	URL Out: Host URL Out: Port URL Out: URI	<p>These fields define the URL to which browsers are redirected for unauthenticated user redirections. The default values reference the NWSP application.</p> <ul style="list-style-type: none"> <li>• Host—Enter the name or IP address for the web server that contains the content application for unauthenticated user redirections.</li> <li>• Port—Enter the listener port number for this content application. The default is the port number you entered for the NWSP application.</li> <li>• URI—The absolute page name you want the subscriber to see. The default is /home, which is the NWSP logon page.</li> </ul>	
Initial Captivation	Enable	Check this box to configure initial logon redirections.	
	Port In	<p>Enter the port that the Captive Portal web server will listen on for initial logon redirections.</p> <p><b>Note</b> You must configure the SSG TCP redirect feature to send initial logon redirections to this port.</p> <p>Default: 8091</p>	
	URL Out: Host URL Out: Port URL Out: URI	<p>These fields define the URL to which browsers are redirected for initial logon redirections. The default values reference the Message Portal application.</p> <ul style="list-style-type: none"> <li>• Host—Enter the name or IP address for the web server that contains the content application for initial logon redirections.</li> <li>• Port—Enter the listener port number for this content application. The default is the port number you entered for the Message Portal application.</li> <li>• URI—The absolute page name you want the subscriber to see. The default is /initial, which is the Message Portal greeting page.</li> </ul>	
	Duration	<p>The length of time that the Message Portal application waits before attempting to redirect the browser to the user's originally requested URL.</p> <p>Default: 15</p>	

Table 5-5 *SESM Installation and Configuration Parameters (continued)*

Category	Input Summary	Explanation	Value
Advertising Captivation	Enable	Check this box to configure advertising redirections.	
	Port In	Enter the port that the Captive Portal web server will listen on for advertising redirections.  <b>Note</b> You must configure the SSG TCP feature to send advertising redirections to this port.  Default: 8092	
	URL Out: Host URL Out: Port URL Out: URI	These fields define the URL to which browsers are redirected for advertising redirections. The default values reference the Message Portal application. <ul style="list-style-type: none"> <li>• Host—Enter the name or IP address for the web server that contains the content application for advertising redirections.</li> <li>• Port—Enter the listener port number for this content application. The default is the port number you entered for the Message Portal application.</li> <li>• URI—The absolute page name you want the subscriber to see. The default is /advertising, which is the Message Portal advertising page.</li> </ul>	
	Duration	The length of time that the Message Portal application waits before attempting to redirect the browser to the user's originally requested URL.  Default: 15	

Table 5-5 *SESM Installation and Configuration Parameters (continued)*

Category	Input Summary	Explanation	Value
Unconnected Service Redirection	Enable	Check this box to configure service redirections, including a default service redirection.	
	Default Service Redirect Port In	Enter the port that the Captive Portal web server will listen on for default service redirections. Default service redirections are used for services whose address does not belong to the destination network of any of the specific service redirections  <b>Note</b> You must configure the SSG TCP feature to send default service redirections to this port.  Default: 8093	
	First Service Redirect Port In Second Service Redirect Port In Third Service Redirect Port In	Enter the ports that the Captive Portal web server will listen on for service redirections for Service1, Service2, and Service3.  <b>Note</b> You must configure the SSG TCP feature to send redirections to these ports.  Defaults: 8094, 8095, 8096	
	URL Out	Enter the URL to which browsers are redirected for any type of service redirection. The default value references the NWSP application, as follows: <ul style="list-style-type: none"> <li>The host and port values are the ones you entered earlier for the service application.</li> <li>The page name is /serviceRedirect, which is a generalized NWSP page. Configuration parameters in nwsp.xml define more specific pages.</li> </ul> This installation program assumes that the same URL is used for all service redirections. You can change this default configuration in the captiveportal.xml file. There is no requirement that all service redirections use the same page, port, or application.	
Details for Service Redirection	Pass Service Names	Choose this option if you want the Captive Portal application to pass the service names to the content application that handles service redirections (NWSP in the default configuration). NWSP uses the service name to connect to the service.  If you do not check this option, NWSP displays the page specified in the serviceNotGivenURI attribute in nwsp.xml. (The default installation setting for the serviceNotGivenURI attribute is the NWSP status page.)	
	Redirect Service Names	Provide the service name as specified in the service profile. The default values provided in the installation program match services in the sample data installed with SESM.	

Table 5-5 *SESM Installation and Configuration Parameters (continued)*

Category	Input Summary	Explanation	Value
If you choose Proxy mode for RDP, then the installation process prompts you for the following RADIUS server information.			
RDP to RADIUS communication	Primary AAA server IP	Enter the IP address or the host name of the primary RADIUS AAA server that you want RDP to communicate with.	
	Primary AAA server port	Enter the port number on the primary RADIUS server host that the RADIUS server listens on.	
	Secondary AAA server IP	Enter the IP address or the host name of the secondary RADIUS server. If you are not using a secondary RADIUS server, enter the same value used for the primary server.	
	Secondary AAA server port	Enter the port number on the secondary RADIUS server host that the RADIUS server listens on. If you are not using a secondary RADIUS server, enter the same value used for the primary server.	
	Shared secret	Enter the shared secret used between RDP and the RADIUS server. The shared secret must be the same for both servers.  The default is <code>cisco</code> .	

The installation program installs the components on your system. When it is finished installing the files, it displays an additional window about modifications to the LDAP directory.

LDAP directory modifications	Extend schema	<p>Choose this option if you want the installation program to apply the SPE schema extensions to the LDAP directory. These extensions include the <code>dess</code> and <code>auth</code> classes and attributes. For more information about the extensions, see the <i>Cisco Distributed Administration Tool Guide</i>.</p> <p>If you do not choose this option, you must extend the directory schema later, before running the SESM application in LDAP mode and before logging into CDAT to create objects in the directory. See the “<a href="#">Extending the Directory Schema and Loading Initial RBAC Objects</a>” section on page 6-40 for more information.</p> <p><b>Note</b> If you are installing the SPE components in multiple locations, you only need to extend the schema one time.</p>	
	Install RBAC	<p>Choose this option if you want the installation program to load the top-level RBAC objects.</p> <p>If you do not choose this option, you must install RBAC objects later, before running an SESM application in LDAP mode and before logging into CDAT to create objects in the directory. See the “<a href="#">Extending the Directory Schema and Loading Initial RBAC Objects</a>” section on page 6-40 for more information.</p> <p><b>Note</b> If you are installing the SPE components in multiple locations, you only need to install the RBAC objects one time.</p>	

# Installation Results

The Cisco SESM installation directory contains the following subdirectories and files:

- `_uninst`—This subdirectory contains the utility to uninstall the components you just installed. To uninstall components, run the executable file in this directory.
- `jetty`—This directory contains the following subdirectories:
  - `bin`—Contains start scripts for Jetty server applications
  - `config`—Contains configuration files that control Jetty servlets
  - `lib`—Contains the Jetty server class libraries.
- `lib`—This directory contains the SESM libraries and the `docs` subdirectory, which contains the Java application documentation.
- `licensenum.txt`—This file contains the license number that you used during installation and the version number of the SESM software that you installed.
- `nwsp`, `pda`, and `wap`—These directories contain the following subdirectories:
  - `config`—Contains configuration files for the portal application and `demo.txt` files.
  - `docroot`—Contains the Web application, including libraries, JSPs, images, and a J2EE configuration file.
- `nwsp311`—Contains the NWSP application from SESM Release 3.1(1). This earlier application is included as a migration tool.
- `redist`—This directory contains libraries from other companies that Cisco is redistributing. It includes the Jasper JSP framework, the JMX framework, and the JAXP XML parser framework. It also includes test tools.
- `captiveportal` and `messageportal`—These directories are included only if you installed the Captive Portal solution using a Custom installation.

When you install SESM in LDAP mode, the installation directory contains the following additional directories:

- `rdp`—This directory contains startup scripts, configuration files, and libraries for the RADIUS/DESS Proxy Server.
- `cdat`—This directory contains configuration files and libraries for CDAT.
- `dess-auth`—This directory contains the SPE DESS and AUTH libraries, SPE DESS schema, and sample data.

## Post-Installation Procedures

This section outlines the steps to take after you successfully complete an installation.

- 
- Step 1 Perform all configuration activities listed in [Table 2-2 on page 2-6](#) (RADIUS mode) or [Table 2-4 on page 2-9](#) (LDAP mode).
  - Step 2 Add configuration information for additional SSGs, if the SSG port bundle host key feature is not used on the SSGs.

The SESM installation program caters to use of a single SSG or multiple SSGs with the host key feature. For multiple SSG support without the host key feature, you must configure the SSG to client subnet mapping. See the [“Associating SSGs and Subscriber Requests”](#) section on page 6-25 for instructions.

- Step 3** (Optional) If you installed the captive portal solution, see the [“Additional Configuration Steps”](#) section on page 8-9 for instructions on configuring an SSG to work with the installed captive portal features.
- Step 4** (Optional) If you installed the RDP server and turned on the restricted client feature, you might need to add more SSGs to the RDP’s client list. The installation program accepts information for one client. You must edit the rdp.xml file to add additional clients. See the useClientList attribute in [Table 6-6](#) on page 6-32.
- Step 5** Start an SESM portal application, start a web browser, and logon as described in [Chapter 7, “Running SESM Components.”](#)
- 

See the [“Configuring a Customized SESM Application”](#) section on page 6-44 for information about configuring a customized SESM portal applications.

